CLAIMS

1. A method of securing communication between a first party and a
second party comprising the steps of:
defining a criteria for selecting one of a plurality of different
security methods, the plurality of security methods each
comprising a plurality of messages selected from a set of
messages, at least two different security methods having at least
one message in common;
    selecting one of the said plurality of different security
methods in accordance with said defined criteria; and
    performing said security method.

2.   A method as claimed in claim 1, wherein said criteria is to
select the security method is selected at random.

3.   A method as claimed in claim 1 or 2, wherein said criteria
is to select said security method based on the processing
capability of the first and/or second party.

4.   A method as claimed in claim 1, 2 or 3, wherein said
criteria is to select the security method in dependence on the
amount of time since the last security method was performed.

5.   A method as claimed in any one of the preceding claims,
wherein said criteria is to select the security method based on
the function provided by the security method.

6.   A method as claimed in any one of the preceding claims,
wherein the plurality of security methods comprise at least one
authentication method and/or at least one rekeying method.

7.   A method as claimed in claim 6, wherein at least one
authentication method includes a key exchange to create a shared
secret.

8.   A method as claimed in claim 6 or 7, wherein a rekeying

method is performed after an authentication method.

9.   A method as claimed in claim 6, 7 or 8, wherein a rekeying method is without carried out without authentication.

10.   A method as claimed in claim 6,7 or 8, wherein the rekeying method is authenticated.

11.   A method as claimed in claim 10, wherein the set of messages includes at least one of the following message types: at least one random number message; at least one hash function message; at least one signature function message; at least one parameter for use with a given function message; at least one security parameter message; at least one key for a given function message; at least one encoded message; at least one message to and/or from at least one third party; and at least one authentication response message.

12.   A method as claimed in claim 11 wherein the set of messages includes the following message types: one signature function message; two security parameter messages; two random number messages; one encoded signature function message; one encoded user identification message; two parameters for use with given function messages; two hash function messages; one contact message with a third party; one response message from the third party; one authentication response message; and two public parameters for the given function.

13.   A method as claimed in claim 12, wherein the set of messages are as follows:

1.   n,g
2.   R
3.   R'
4.   P
5.   P'
6. $g^x \bmod n$
7. $g^y \bmod n$
8.   hash[SIG 1] (n|g|g^x|g^y|g^{xy}|P|P'|R|R'|B)
9.   hash[SIG 2] (n|g|g^x|g^y|g^{xy}|P|P'|R|R'|B|U)
10. SIG_B (hash[SIG1]n|g|g^x|g^y|g^{xy}|P|P'|R|R'|B)

11. $E_k(SIG_u(hash[SIG2](n|g|g^x|g^y|g^{xy}|P|P'|R|R'|B|U)))$
12. $E_k(S_U)$
13. $hash[AUTH](n|g|g^{xy} mod\ n|R|R'|B|U),\ U$
14. $hash[RESP](hash[SEC]S|hash[AUTH](n|g|g^{xy} mod\ n|R|R'|B|U))$
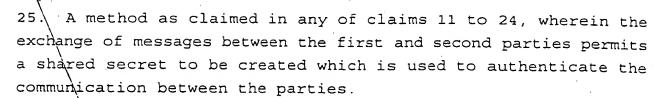15. $hash[SEC](S|hash[AUTH](n|g|g^{xy} mod\ n|R|R'|B|U))$

where n and g are Diffie Hellman public parameters, R and R' are random numbers, P and P' are security parameters, g is a generator of the Diffie Hellman exchange, x and y are random exponents, n is the modulus of the Diffie Hellman key exchange, B and U are the identity of the first and second parties, SIG represents a signature, E_k represents encryption, AUTH represents authentication.

14. A method as claimed in claim 11, 12 or 13, wherein a first security method uses the following messages: the first and second keys for a given function messages; first and second random number messages, first and second security parameter messages, a signature function message, one encoded user identification message and optionally at least two parameters for use with a given function message.

15. A method as claimed in claim 11, 12, 13 or 14 wherein a second security method uses first and second random number messages, first and second security parameter messages, first and second keys for a given function messages, a signature function message and optionally first and second parameters for use with the given function message.

16. A method as claimed in any of claims 11 to 15 wherein a third security method uses first and second random number messages, first and second security parameter messages, first and second keys for given function messages, one encoded user identification message, one message to and one message from a third party, one authentication response message and optionally first and second parameters for use with a given function message.

17. A method as claimed in any of claims 11 to 16 wherein said

security method is a first rekeying method and comprises first and second random number messages.

18. A method as claimed in any of claims 11 to 17 wherein the security method is a second rekeying method and uses first and second random number messages and first and second hash function messages.

19. A method as claimed in any of claims 11 to 18 wherein the security method is a third rekeying method comprising first and second random number messages, a signature function message and an encoded message.

20. A method as claimed in any one of claims 11 to 19, wherein one security method is a fourth rekeying method and comprises the use of first and second random number messages, one message to and one message from the third party and one authentication response message.

21. A method as claimed in any of claims 11 to 20, wherein the given function is a Diffie-Hellman function.

22. A method as claimed in any of claims 11 or 22, wherein at least one of said messages types comprises two messages, one message being from the first party and the other message being from the second party.

23. A method as claimed in any of claims 11 to 22, wherein the encoded message is used to transfer information as to the identity of at least one of the first and second parties to the other of the first and second parties.

24. A method as claimed in any of claims 11 to 24, wherein at least one of said first and second parties is arranged to communicate with a trusted third party and is arranged to receive messages from and/or send messages to that trusted third party.

25. A method as claimed in any of claims 11 to 24, wherein the exchange of messages between the first and second parties permits a shared secret to be created which is used to authenticate the communication between the parties.

26. A method as claimed in claim 6 or any claim when appended to claim 6, wherein at least one rekeying method comprises the steps of exchanging at least one random number between the first and second parties.

27. A method as claimed in claim 26, wherein at least one of the random numbers is authenticated.

28. A method as claimed in any preceding claim, wherein the method is used in a telecommunications network.

29. A method as claimed in claim 28, wherein at least one of said first and second stations comprises a mobile station.

30. A method as claimed in claim 28 or 29, wherein at least one of the first and second stations comprises a base station.

31. A wireless telecommunication system comprising a first station and a second station, wherein communication between said first and second station is secured in accordance with the method described in any one of the preceding claims.

32. A network element for securing communication between a first party and a second party comprising:

     means for defining a criteria for selecting one of a plurality of different security methods;

     selection means for selecting one of said plurality of different security methods in accordance with said defined criteria; and

     means for ensuring that the communication between said first and second parties is in accordance with said selected security method.